# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 05-04-2009 | FINAL | |

**4. TITLE AND SUBTITLE**

*Don't Forget The Cyber!* Why the Joint Force Commander must integrate cyber operations across other war fighting domains, and how a Joint Forces Cyberspace Component Commander will help

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

**Martin Stallone, Major, USAF/NYANG**

Paper Advisor (if Any): **CAPT Stephanie Helm**

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution Statement A: Approved for Public Release.

**13. SUPPLEMENTARY NOTES** A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Air Force.

Amidst a geometric increase in the interconnectedness of our world, the official Department of Defense definition calls 'cyberspace' a *global domain* in which all military departments and combatant commands need to operate unimpeded. Despite the operational implications of this statement, there is little published research about how the current Unified Command Plan affects the integration of cyber operations with actions in other domains in the geographic commands. This paper finds U.S. STRATCOM's monopoly over planning and execution of cyberspace operations, as well as the structure and composition of the geographic command that must integrate cyberspace operations at the operational level, suboptimal to creative operational design and integrated force employment. As a remedy, this paper asserts an empowered Joint Force Cyber Component Commander (JFCyCC) within each geographic combatant command will improve the integration of operations in cyberspace with operations in other domains and across the range of military operations. A JFCyCC will enhance the Joint Force Commander's (JFC) freedom of action and military advantage by widening the canvass on which he can creatively paint his forces.

**15. SUBJECT TERMS**

**Cyberspace, Operations in Cyberspace, Joint Task Force (JTF), Cyber Operations, Joint Force Commander (JFC), Domain, Joint Force Cyberspace Component Commander (JFCyCC)**

| 16. SECURITY CLASSIFICATION OF: UNCLASSIED | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Chairman, JMO Dept |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | None | 30 | 19b. TELEPHONE NUMBER *(include area code)* 401-841-3556 |

**Standard Form 298 (Rev. 8-98)**

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# *Don't Forget The Cyber!*
## Why the Joint Force Commander must integrate cyber operations across other war fighting domains, and how a Joint Forces Cyberspace Component Commander will help

**by:**

**Martin Stallone**

**Major, Air Force, New York Air National Guard**

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**Signature: _____**

**May 4, 2009**

.

## Table of Contents

## List of Illustrations

**Abstract**

Amidst a geometric increase in the interconnectedness of our world, the official Department of Defense definition calls 'cyberspace' a *global domain* in which all military departments and combatant commands need to operate unimpeded. Despite the operational implications of this statement, there is little published research about how the current Unified Command Plan affects the integration of cyber operations with actions in other domains in the geographic commands. This paper finds U.S. STRATCOM's monopoly over planning and execution of cyberspace operations, as well as the structure and composition of the geographic command that must integrate cyberspace operations at the operational level, suboptimal to creative operational design and integrated force employment. As a remedy, this paper asserts an empowered Joint Force Cyber Component Commander (JFCyCC) within each geographic combatant command will improve the integration of operations in cyberspace with operations in other domains and across the range of military operations. A JFCyCC will enhance the Joint Force Commander's (JFC) freedom of action and military advantage by widening the canvass on which he can creatively paint his forces.

## INTRODUCTION

Cyberspace is the nervous system of American Society.[1] Nearly every aspect of our modern world, including critical infrastructure and information, is interconnected by computer networks. Moreover, information technology is advancing rapidly, and the number of people connected in cyberspace continues to grow exponentially.[2] Cyberspace simultaneously bestows power and vulnerability on those it connects. The U.S. government understands that various technologies, such as communication and control systems, are critical to a nation's ability to deploy and sustain military forces, and are accessible through cyberspace.[3] Hence, the Department of Defense (DoD) has identified cyberspace as "critical to the conduct of military operations around the globe."[4] Cognizant of the importance of cyberspace, this paper asserts a standing *Joint Force Cyber Component Commander* (JFCyCC) in each geographic combatant command (GCC) will improve the integration of cyberspace operations with efforts in other domains across the range of military operations. This resource will increase the freedom of action and military advantage of a Joint Force Commander (JFC) in support of GCC objectives, by not only widening the canvass on which he creatively paints his forces, but also by expanding his color palette.

This recommendation follows DoD's declaration that cyberspace is a *global domain,* analogous to land, sea, air and space, where U.S. forces must be able to operate unhindered.[5] The 2008 Unified Command Plan (UCP) updated responsibility for "cyberspace operations"

---

[1] U.S. President, *The National Strategy to Secure Cyberspace.* (White House, Washington, DC: 2003)
[2] CNO SSG 27, *Collaborate & Compel—Maritime Force Operations.* (Report to the CNO: July 2008), 9.
[3] U.S. General Accounting Office, *Information Security—Computer Attacks on the Department of Defense Pose Increasing Risks.* (Washington DC: Government Printing office, 1996). Chapter 0:0.3
[4] U.S. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations (NMS-CO)* (U), (Washington, DC: CJCS, September 2006) vii.
[5] U.S. Office of the Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Memo, 12 May 2009.

to U.S. Strategic Command (STRATCOM).[6] In this important warfighting domain, STRATCOM'S monopoly over planning adversely affects the integration of cyberspace operations with efforts in other domains at the operational level of war. With no empowered advocate for cyberspace operations in the geographic combatant commands, the planning process is deprived of cyberspace expertise that focuses solely on operational missions. A JFCyCC who advocates for integrated cyberspace operations that accomplish operational objectives would correct this shortcoming.

## DEFINING CYBERSPACE FOR OPERATIONAL PURPOSES

Despite DoD's general acceptance of its importance, consensus on how cyberspace should be regarded for military operations is a work in progress. The road to the current definition (as stated by the Deputy Secretary of Defense in June 2008) was long and arduous. "Cyberspace" was first coined in 1984 by William Gibson in his novel, Neuromancer. It calls cyberspace a "consensual hallucination."

> …A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding.[7]

Since 1984, dozens of definitions have attempted to capture the essence of cyberspace.[8] Most definitions are skewed toward how the defining party uses cyberspace. Gibson, for example, defined cyberspace in the context of children playing video games. The wide range of proposed definitions indicates cyberspace plays a key role in many human activities including economic exchanges, social communication, and war. The military enterprise is a special case, in which definitions are more than just descriptive. They also instruct capability development, and how capabilities are employed. This is why the services

[6] U.S. Department of Defense. *DoD Releases Unified Command Plan 2008*. News Release. December 2008.
[7] Gibson, William. *Neuromancer*. (NY, New York: Ace Books, 1984), 69.
[8] CNO SSG XXVI. *Convergence of Sea Power and Cyber Power*. (Report to CNO: 13 July 2007), 8-10.

require a cyberspace definition that is helpful in framing the conduct of operations in cyberspace for military advantage, while at the same time instructive to program development, useful for acquisitions, etc. By 2006, DoD achieved the important milestone of a common cyberspace definition that designated it a warfighting "…*domain* characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[9] Previously, there was dispute about whether cyberspace is best described as a "domain", rather than a "space", an "environment," or something else.[10] Following a more restrictive definition of cyberspace in National Security Presidential Directive-54 (which omitted calling cyberspace a domain), the Deputy Secretary of Defense, Gordon England, relabeled cyberspace a warfighting domain.[11] He also declared his to be the official definition of cyberspace "until further notice."[12]

Each of the major definitions presented imply cyberspace comprises a part of the "physical and information dimensions" of the larger "information environment."[13] The portion of the information environment that cyberspace comprises is also where Computer Network Operations (CNO) occurs, as defined in Joint Publication 3-13.[14] This relationship is depicted in Figure 1 in the appendix. Although cyberspace was not always regarded as a domain, this is now an integral aspect of the definition.

Although the word is used frequently throughout the joint publication series, "domain" is not explicitly defined there. Professor Milan Vego explains a domain as a "sphere of

[9] U.S. Office of the CJCS. *NMS-CO*. 2006. ix.
[10] Daniel Kuehl. *From Cyberspace to Cyber Power.* (NDU Working Paper, Washington. D.C., 2006), 2-6.
[11] U.S. President. *National Security Presidential Directive 54 (NSPD-54).* (White House, Washington, DC: 2008), and U.S. Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Letter, 12 May 2009.
[12] U.S. Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Dated 12 May 2009.
[13] U.S. Army, *IO Primer. Fundamentals of IO.* (U.S. Army War College. Carlisle, PA. Dec. 2007), 2.
[14] U.S. Office of the CJCS. *Information Operations*. Joint Publication (JP) 3-13. (Washington, DC: CJCS, 13 Feb 2006.) II, 4-5.

activity, concern, or function or a field."[15] Webster's dictionary defines it as "territory over which dominion is exercised," and "a region distinctively marked by some physical feature."[16] Without philosophical arguments, let it be sufficient to understand a "domain" as a physical phenomenon where someone can perform activities and create effects. However, the operational implications of the word "domain" deserve amplification.

## OPERATIONAL IMPLICATIONS OF THE CYBERSPACE "DOMAIN"

The physical aspects of a domain delineate and constrain how humans act there. In order to perform activities and create certain effects, humans sometimes need machines, electronics or other technology. In general, technology allows an expanded, but not infinite repertoire of actions. This is true for all domains. In space, technology is needed to do practically anything. In the other traditional physical domains, humans use technology to enhance natural actions and their effects. Consider how our natural ability to move and lift objects on land is expanded with the assistance of technologies such as engines and hydraulics. Likewise, use of the ocean requires ships and submarines to do more than swim. The physical aspect of cyberspace is the "interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[17] Within this network, electrons and the electromagnetic spectrum are *what* humans use to act, while effects achieved depend on *how* they are used.[18]

Domains are places where different human activities occur that cause effects. For example, the air domain hosts activities as diverse as scientific experiments (weather

[15] Milan Vego. *Joint Operational Warfare: Theory & Practice*. (Newport, RI: Naval War Press, 2007), XIII-31.
[16] Webster's Dictionary, "*Domain*" http://www.merriam-webster.com/dictionary/domain (accessed 28 Apr 2009)
[17] U.S. Office of the Deputy Sec Def. *The Definition of "Cyberspace."* Policy Letter, 12 May 2008.
[18] Convertino, et. al. *Flying and Fighting in Cyberspace.* (Paper # 40. Maxwell, AL: AU Press, July 2007), 7.

balloons), hand gliding, commercial air travel and bombing missions. Likewise, cyberspace can be used for social, economic, military, educational and other purposes. Within and across domains, different combinations of actions may achieve the same effect. Cyberspace offers new and unique ways to access a party of interest and affect them.

Cyberspace overlaps with other physical domains, as depicted in figure 2 in the appendix. Entry and exit points of cyberspace can exist practically anywhere. This construct is useful to an operational planner because a JTF, for example, organizes force by domain.[19] Along with air, sea and land component commanders acting in their domains, a cyber component commander would determine which actions in cyberspace were advantageous, while understanding which enemy actions could threaten operational success. One can imagine innumerable cross-domain operations in which a connected person in one physical domain causes effects (by acting through cyberspace) at a remote location where cyberspace interfaces with a second domain. To demonstrate this concept, consider the following hypothetical cross-domain operation that facilitates enemy access for military advantage.

An insurgent hideout in Iraq is targeted by air strike. Concurrently, cyberspace operations monitor patient census at the nearest hospital in real-time and notice several burn patients arrive at the hospital soon after the strike. These patients are unknowingly connected to U.S. forces through cyberspace. Army infantrymen are directed to conduct physical surveillance and they track the men who brought the insurgents to the hospital back to their homes. Phone pattern analysis of those houses reveals heavy call volume to several nearby locations. Ground forces raid these homes and capture sixteen additional suspects for

[19] Kelly L. Olsen, *Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative*. (research paper, Carlisle Barracks, PA: U.S. Army War College, 2008), 2-3.

questioning. Efforts across the air, land, and cyber domains yielded better outcomes than operations in any single domain could yield alone.

Extrapolating from standard actions in the traditional domains, a Joint Force Commander may envision (or be advised about) operational functions in the cyber domain that support operational objectives. This includes the joint functions of operational maneuver, fires, protection, C2, etc. Operations in cyberspace can be joint or combined if the capabilities brought to the conflict are developed or supplied by different services or nations. For example, British special operations teams might access enemy closed networks to allow U.S. Navy cyber warrior experts to remotely manipulate power grids or communication systems for coalition military advantage.

Like the other domains, cyberspace is global. It is unique, however, because it enables instantaneous global reach—necessitating a careful consideration of the factors of time and space when seeking to cause or avoid effects through cyberspace. It is also unique because most modern military operations across all other domains are coordinated, synchronized, and integrated through cyberspace. Our highly networked world has inexorably linked the cyber domain to operations whose nature, at first glance, appear purely "land" or "maritime."

Perhaps the most important point about the cyberspace domain for the military is related to how many different critical aspects of our society are interconnected. The ability to influence through cyberspace hinges on connectedness, and the number of connections in cyberspace is growing exponentially.[20] The next decade is expected to see the interconnection of a wide array of electronic devices and machines. In that environment, instantaneous global connectedness through cyberspace imparts both a power and vulnerability—all aspects of society are potential military targets, not just what is near the battlefield. The computers used

[20] CNO Strategic Studies Group XXVII. *Collaborate & Compel*. Final Report, 9-12, 19.

as weapons are indistinguishable from those used for peaceful purposes, until they attack. The cyber-artillery (software) is easily accessible, and often free. Counterattacks can be directed on targets far away from where the initial attack occurred, and attribution is frequently difficult. Access to information will empower new groups to achieve impressive effects with meager resources.

Nothing written about cyberspace thus far erases the JFC's fundamental responsibility to integrate ends, ways, and means to achieve the operational objectives of the mission. Commanders and staffs apply operational art during operational design to "visualize the arrangement of joint capabilities in time, space, and purpose" to defeat an adversary.[21] The essence of operational art—and fundamental to joint warfare—is the holistic assessment of friendly and enemy forces across domains and the subsequent creative arrangement of forces to gain military advantage, and achieve objectives.[22] The commander's *operational vision* must encompass cyberspace, even if he is not experienced in such operations.[23]

Professional military officers identify and study predecessors who exhibit broad operational vision.[24] In describing military genius, Carl von Clausewitz speaks of c*oup d'oeil*, or "the talent great men have in conceiving in a moment all the advantages of the terrain and the use they can make of it with their army."[25] Drawing from our nation's war experience, we invoke George Patton pushing toward Germany, William Halsey maneuvering in the Pacific Ocean, and Carl Spaatz bombing Europe from the sky. Each man understood his domain, and operated in it for military advantage. Perhaps textbooks will describe

[21] CJCS. *Joint Operations*. Joint Publication (JP) 3-0. (Washington, DC: CJCS, 13 February 08), xix
[22] Ibid
[23] Milan Vego. *Joint Operational Warfare*, X1-35
[24] Ibid
[25] Ibid, X1-37

accomplishments in cyberspace in a similar light someday. As airpower was showcased in Operation DESERT STORM in 1991, perhaps the Long War will see the application of overwhelming cyber power "compel our enemy to do our will."[26]

This begs the question: Are there *cyber-operational-artists* in our ranks ready to leave their mark on the history of warfare? Is cyberspace sufficiently understood for a military planning group to envision integrating the cyberspace domain with others to optimize forces in space and time? What are the consequences of being unprepared? Command relationships must encourage successful operational design and integrated force employment. The value of a cyberspace component commander, therefore, must be framed in terms of its effect on operational art and operational design at the level of a combatant command or JTF, and in the context of the current paradigm of cyber operations.

## ANALYSIS OF THE CURRENT PARADIGM OF CYBERSPACE OPERATIONS

Cyberspace operations are performed by forces assigned to a combatant command and supported by various combat support agencies, such as the National Security Administration (NSA). Today, "cyberspace operations" are synonymous with Computer Network Operations (CNO) and include computer network exploitation (CNE), defense (CND) and attack (CNA).

Computer Network Exploitation (CNE) and Signals Intelligence (SIGINT) are performed by NSA in Ft. Meade, MD.[27] NSA's workforce represents an unusual combination of specialties: engineers, physicists, analysts, mathematicians, linguists, computer scientists, researchers and data flow experts.[28] CNE and intelligence, surveillance, and reconnaissance (ISR) in cyberspace involves determining adversary cyberspace identities and capabilities. It assists in planning of successful cyber defenses and attacks. This is a time consuming and

[26] Carl Von Clausewitz, *On War*, translated by Peter Paret (NJ: Princeton University Press, 1976), 75.
[27] U.S. Army, *IO Primer*, 15.
[28] Ibid

technical activity that is completed largely by civilians and military in title 50 legal status. Title 50 law deals with war and national defense, including foreign intelligence gathering. Computer Network Exploitation (CNE/ISR) enables Computer Network Attack (CNA) which is a title 10 military activity, pertaining to the use of armed forces. The CNA planning mission is assigned to the Joint Functional Component Command for Network Warfare, (JFCC/NW), which is a subordinate command of STRATCOM. The person filling the position of the Director of NSA (DIRNSA) is also designated the Commander of JFCC/NW and serves as a link between Title 50 and Title 10 cyberspace activities. Computer Network Defense (CND), supported by NSA and JFCC/NW, is primarily accomplished by STRATCOM's Joint Task Force for Global Network Operations (JTF-GNO).

According to the UCP, the national command authority assigns cyberspace forces to combatant commanders based on the envisioned cyber forces necessary for the mission. There are four general patterns of cyberspace force allocation and command relationships based on the nature of the mission, although exceptions exist.[29] First, combatant command (COCOM) of cyber forces is granted to a functional command with global authority for global missions (i.e. STRATCOM). Second, COCOM of cyber forces is assigned to a geographic command (GCC) for regional missions. Third, for missions that require temporary but sole use of resources for a limited time, operational or tactical control of cyber forces is assigned to a GCC. Forces are provided by the services or U.S. Joint Forces Command (JFCOM), the UCP-designated force provider. Fourth, cyber forces from STRATCOM can *support* regional missions that require only *shared* cyber resources for a limited time. These are missions without a significant cyberspace aspect. However, for all cyberspace operations, STRATCOM is the UCP-designated supporting commander for planning and execution.

[29] U.S. Air Force Cyber Command, *Concept of Cyber Warfare*, 15.

For missions expected to require only shared cyber resources for a limited time, the quality of operational design and integration of cyberspace operations with efforts in other domains is diminished. The problem is that STRATCOM must simultaneously balance resources, effort and attention between its global mission and the regional missions it supports. In a supporting role, JFCC/NW may not understand the nature of a regional mission to the same extent a JTF staff does. Even if it did, the cyber force commander does not own the mission. Here, unity of effort is by *cooperation*. This operational command organization is suboptimal. Prof. Vego explains, "the highest degree of effectiveness is ensured by having unity of effort through unity of command."[30] Unity of effort in cyberspace is cumbersome when both strategic and operational actions are orchestrated from a strategic position.

Perhaps a false premise, do missions that "require only shared cyber resources for a limited time" even exist? In planning to use military force, one must remember that cyberspace, which is global in nature, supports all other warfighting domains, including air, land, maritime and space, with offensive and defensive capabilities. Cyberspace operations, including network defense, exploitation, and attack, protect freedom of action in cyberspace and significantly enhance the effectiveness of military operations across the board.

Besides the challenge of balancing priorities between combatant commands, the typical joint staff composition and structure in a GCC provides insufficient advocacy for cyberspace operations in contingency, crisis, and theater security cooperation planning. For each activity, the true shortcoming is not fully exploring how operations in cyberspace might synergize with operations in other domains to best achieve operational objectives. Neither the staff structure, nor how it interfaces with STRATCOM, facilitates this endeavor.

[30] Milan Vego, *Joint Operational Warfare*, VIII-13.

As JP 3-13 describes, STRATCOM assigns JFCC/NW liaisons to the JFC staff to coordinate cyber operations with operational planners as part of the Information Operations (IO) Cell.[31] Here, advocacy for cyberspace operations and information operations are comingled, even though they are not equivalent.

Information operations is the use of specific capabilities (Electronic Warfare, CNO, Psychologic Operations, Military Deception, and Operational Security) "to influence, disrupt, corrupt or usurp adversarial human and automated *decision making* (emphasis added) while protecting our own."[32] IO is used for operational missions, whereas cyberspace describes a domain in which to operate. IO can be performed in any domain, including cyberspace. An airplane dropping leaflets with a message aimed to influence an audience is conducting IO (psychological ops) without using cyberspace. Similarly, operations in cyberspace are not limited to IO. Manipulating an enemy airport computer system to disable the fuel pumps is a cyberspace operation, but not an example of IO.

Therefore, it is imprecise to equate all cyber operations with information operations. An advocate for IO is technically outside his field of expertise to advocate using cyberspace for purposes other than to "influence, disrupt, corrupt or usurp adversarial human and automated decision making or protect his own." Likewise, a strict cyber perspective omits IO actions outside cyberspace. Moreover, operations in cyberspace should be coordinated and synchronized both tactically and operationally with the operations in the other domains. This should be accomplished at the operational level, and not the strategic level of war.

With the exception of cyberspace, each of the warfighting domains has a primary component commander to discern how operations therein can help achieve mission

[31] CJCS, *Information Operations*, JP 3-13, IV-4.
[32] Ibid, ix.

objectives. As one author pointed out, "Though each service shares time and space in every combat domain, each service jealously covets their respective primary warfighting domain."[33] Mislabeled a subset of IO, cyberspace capabilities outside those brought by the service components are handled by the IO Cell. This is an integrated working group under the operations directorate that touches all elements of the staff and beyond, to include interagency, multinational partners, and relevant civilian entities.[34] Although it has far reaching relationships, the IO Chief (typically J39, under the J3) is designated only as a *coordinating authority* between the representatives in a typical IO Cell.[35] With few exceptions, most of these members are not permanent staff members. JP 1-0 explains coordinating authority as "authority to require consultation between the agencies involved, but [not] authority to compel agreement…[this] authority is more applicable to planning and similar activities than to operations."[36] Unlike land or maritime forces, cyberspace forces often come from outside the GCC in a manner that is secretive, poorly integrated, and confusing to those at the operational level. The former STRATCOM commander admitted:

> Cyber operations [are] often cloaked behind a lot of green doors and 'I can't tell you this' and 'I'd like to tell you that'… [We] set expectations that are probably unrealistic…We launch "recce teams" out to see what's going on…we build a couple of attack teams over here, we make sure the "recce teams" don't tell the defenders what they found, or the attackers, and the attackers go out and attack and don't tell anybody that they did. *It's a complete secret to everybody in the loop and it's dysfunctional. It's really got to change*.[37]

Although the JFC has authority to direct integration of cyberspace operations that support the mission, such operations are not intuitive to everyone. This is why the operational

---

[33] Kelly L. Olsen, *Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative*. (research paper, Carlisle Barracks, PA: U.S. Army War College, 2008), 1.
[34] CJCS, *Information Operations*, JP 3-13), IV-4.
[35] Ibid
[36] U.S. Office of the CJCS. *Doctrine for the Armed Forces of the United States*. Joint Publication (JP) 1-0. (Washington, DC: CJCS, 20 March 2009), IV-13.
[37] James Cartwright. *Striking the Balance-Today's War, Tomorrow's Threats, Future Technology.* Address to AFA Symposium, Orlando, FL, 8 Feb 2007.

level needs an empowered advocate who can understand and articulate cyberspace operations in terms of their anticipated effects. Currently this is an expectation of the J39 in each GCC.

The J39 is responsible for the five core capabilities of information operations. The complexity of cyberspace operations demands more attention and expertise than what the J39 typically provides. The director of human resources for J3 at CENTCOM, confirmed the current J39 has no formal experience at NSA or STRATCOM, but does have information operations experience.[38] The former Deputy Chief of Operations (J3A) of JFCC/NW explained that while geographic combatant command J39s are responsible for information operations, they, for the most part, do not plan and execute cyberspace operations. For example, cyberspace defense at the geographic combatant commands generally falls to the J6 who usually only focuses on that aspect of cyberspace operations and, therefore, has a poor understanding of cyberspace operations in total.[39] However, because IO includes computer network operations, JP 3-13 asserts the J39 can plan for CNO. However, the operational level needs a more integrated approach to cyber-effect management.

Planning, integrating, deconflicting and executing cyberspace operations involve multiple services, DoD agencies, and other partners. Recognizing and understanding the mutually supporting nature of the network warfare disciplines of network exploitation, defense and attack, and of the various organizations involved, is necessary for effectively employing cyberspace operations.[40] Therefore, staff advocacy for planning and integration of forces in cyberspace is insufficient; the J39 may not have the specific expertise this requires.

In light of how cyberspace is understood as a warfighting domain, the current paradigm of cyberspace operations is problematic for two reasons. First, those tasked with

[38]. Telephone interview between author and CENTCOM J3 HR Manager on 27 Apr 09.
[39] Forbes O. MacVane, USN. Fmr. JFCC/NW Dep Chief of Ops (J3A). Personal interview with author 9 Apr 09.
[40] Ibid

the mission receive dual-tasked cyber forces in a cross-combatant command relationship. In other words, the COCOM cannot plan and execute its own cyber effects. Second, the position in the GCC staff currently expected to plan and integrate cyberspace operations is insufficient. They have competing responsibilities, are often outside their area of expertise, and are inferior to the component commanders. This results in suboptimal operational design and planning for integration of cyberspace operations with efforts across the other warfighting domains. This, in turn, threatens mission accomplishment and must be corrected.

## RECOMMEND A JOINT FORCE CYBER COMPONENT COMMANDER (JFCyCC)

The challenges outlined in the preceding section are mitigated if a standing Joint Forces Cyber Component Commander (JFCyCC) is established in each Geographic Combatant Command. This position would provide theater support for the JFC, and could support multiple JTFs as they are established. Meanwhile, in peacetime, it would be planning and supporting IO and would help with immediate crisis action if and when a JTF is required.

Each Geographic Combatant Command, supported by the JFCyCC, could conduct theater-specific preparations for the employment of operations in cyberspace. This position determines how best to integrate assigned and supporting forces. Through a planning process that is informed by a cyberspace advocate, the correct cyberspace resources can be requested. The general goal is to build "corporate knowledge" within the GCC to assist and, if necessary, guide a JTF when formed. A theater cyber security cooperation addendum might accompany the Theater Cooperation Security Plan (TSCP) to guide long term, interagency cooperation through cyberspace. Operational Plans should include detailed cyberspace component instructions and address joint cyber functions. Ongoing refinement of theater CNE requirements would improve targeting for a range of desired effects. The JFCyCC requires

special experiences and skill sets. Broadly, the position requires familiarity with the employment of force and strategic initiatives in cyberspace.

The value of the cyber component to a JFC is the establishment of freedom of action in cyberspace. The JFCyCC would be tasked to properly integrate cyber capabilities across other domains for the purpose of operational objectives. Novel ideas may emerge from integrating and combining efforts across several domains. For instance, a JFCyCC may seek effects involving control systems through cyberspace to combine with capabilities from the air or land components in the same joint operating area. With a better estimate of the risk of unintended strategic effect and cyberspace fratricide, and a specific understanding of the operational effect on the adversary, the JFCyCC would have the authority to champion those cyber operations that best support JTF objectives. An empowered JFCyCC focused squarely on JTF objectives can present options in cyberspace that maximize overall mission success.

The strongest counterargument to a JFCyCC is the need for STRATCOM to retain control over cyberspace operations at the strategic level, across geographic commands to deconflict operations from the top down. This argument rests on the global nature of cyberspace; it is challenging for a geographic command to manage effects that do not respect boundaries. Some might feel the JFCyCC weakens STRATCOM's authority over cyber operations. In rebuttal, a JFCyCC will not infringe on STRATCOM's role in cyberspace operations. Rather, a cyberspace advocate with a mission-tailored perspective at the operational level will enhance the usefulness of STRATCOM's support.

Beyond improving coordination, a JFCyCC might enable STRATCOM to cautiously delegate authority over cyber operations to the operational level. A principle argument for STRATCOM's control of cyberspace operations is the inability of an individual GCC to

handle the strategic aspects of network operations. Capable JFCyCCs could change this assessment. Furthermore, advancements in information technology may enable the JFC to command CNO without risk of unintended consequences. This is true today for the subset of computer network operations with well-defined effects, such as control system attack.[41]

Figure 4 depicts a proposed C2 diagram that explains the relationships between a GCC and STRATCOM pertaining to the JFCyCC. The JFCyCC position should have command authority (at least TACON) over cyberspace forces if any are assigned. Though a component commander under the GCC, it can hold an equivalent function in a JTF, if one is established.

Before establishing a JFCyCC, certain issues must be addressed; though solving them is outside the scope of this paper. An example of such an issue is the ambiguous limits of responsibility in cyberspace. Does the establishment of a JFCyCC imply every action in cyberspace be shifted under the purview of the Cyber Component Commander? Clearly, that is an implausible proposition. But, what would a cyber component command do in relation to the other components commanders? Where, exactly, do the JFCyCC's responsibilities in cyberspace end and another commander's begin? Since cyberspace overlaps all other domains, even classic "land" and "sea" capabilities rely heavily on cyberspace.

Although there will be disputes at the margin, a logical rule is that the JFCyCC commands efforts in cyberspace where full freedom of action is disputed. This is demonstrated in figure 5, which depicts adversaries contesting friendly action in cyberspace. In this case, the JFCyCC coordinates and synchronizes efforts to counter the adversary, and thereby achieves freedom of action in cyberspace. So, as long as there is no contest over cyberspace, the use of cyberspace can be entirely delegated to any component commander for

[41] Mark J. Matsushima, "*Words Mean Things: The Case for Information System Attack and Control System Attack*" (research paper, Newport, RI: U.S. Naval War College, JMO Department, 2008), 5-6.

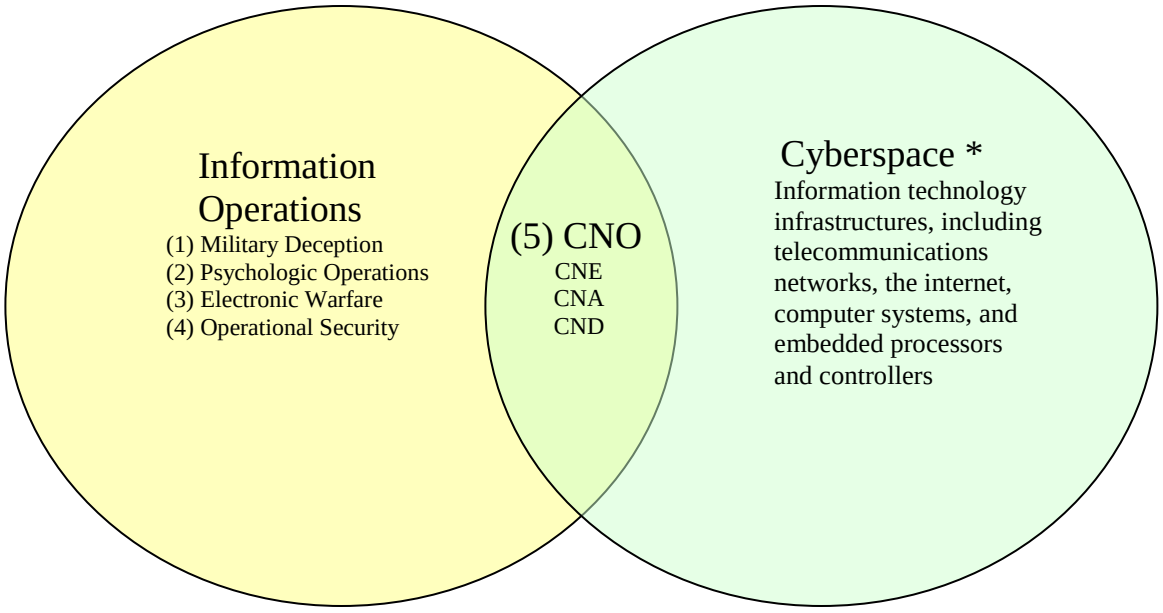
their own purposes. For example, if a pilot fully controls a UAV and radios have unimpeded links, then the system in question can be controlled by the JFACC. However, whenever competing in cyberspace to gain freedom of action, the JFCyCC must be involved so that all necessary cyber resources are brought to bear to gain cyberspace control. Imagine the JFCyCC establishing and maintaining connections into a domain, through which separate experts perform actions to achieve the ultimate effect. This "value chain" requires joint effort and teamwork.[42] Such cross-domain effort must be co-handled by both cyber and other components. Cyberspace is a valuable domain for a Joint Commander to thoughtfully consider when applying operational art to his designs in the joint operational planning process. The JFCyCC argument can be framed in terms of *command organization,* as articulated by Professor Vego.[43] This element of the GCC organization will help ensure the most effective employment of U.S. forces to accomplish mission objectives.

## CONCLUSION

On a tactical level, operations in cyberspace are technical endeavors that require highly trained technicians. However, in modern warfare, operational success achieved by a principal reliance on advanced technologies is rare—especially in a conflict between two strong opponents.[44] More important than technical skill, it is the artful integration of operations in cyberspace with operations in other domains that will generate advantage and increase the likelihood of mission success. To this end, a JFCyCC with equivalent authority to the air, sea, and land component commanders must partake in the planning, preparation, conduct, and sustainment of campaigns and major operations designed to accomplish a JTF's operational objectives in a given theater or Joint Operations Area.

[42] Michael Porter, *What is Strategy*. Harvard Business Review. (Harvard Press. Cambridge, MA, 1996), 61-78.
[43] Milan Vego, *Joint Operational Warfare: Theory & Practice*, VIII-7
[44] Ibid, I-3

**FIGURE 1: INFORMATION OPERATIONS AND CYBERSPACE OVERLAP IN THE AREA OF COMPUTER NETWORK OPERATIONS (CNO), AS PER JP 3-13, *INFORMATION OPERATIONS***

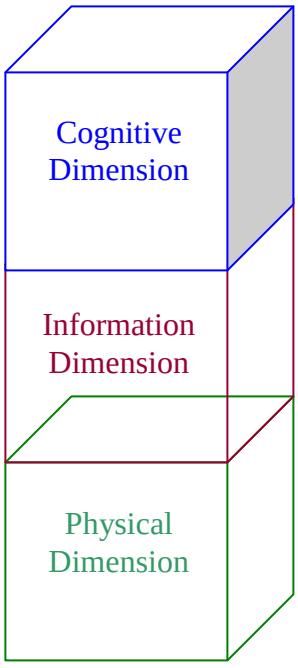



CNO = Computer Network Operations
CNE = Computer Network Exploitation
CNA = Computer Network Attack
CND = Computer Network Defense

* From U.S. Deputy Secretary of Defense. *The Definition of "Cyberspace."* Policy Letter Dated 12 May 2009.

**FIGURE 2: CYBERSPACE IN RELATION TO THE INFORMATION ENVIRONMENT**[45]

**The Information Environment**, consists of the physical, information, and cognitive dimensions.

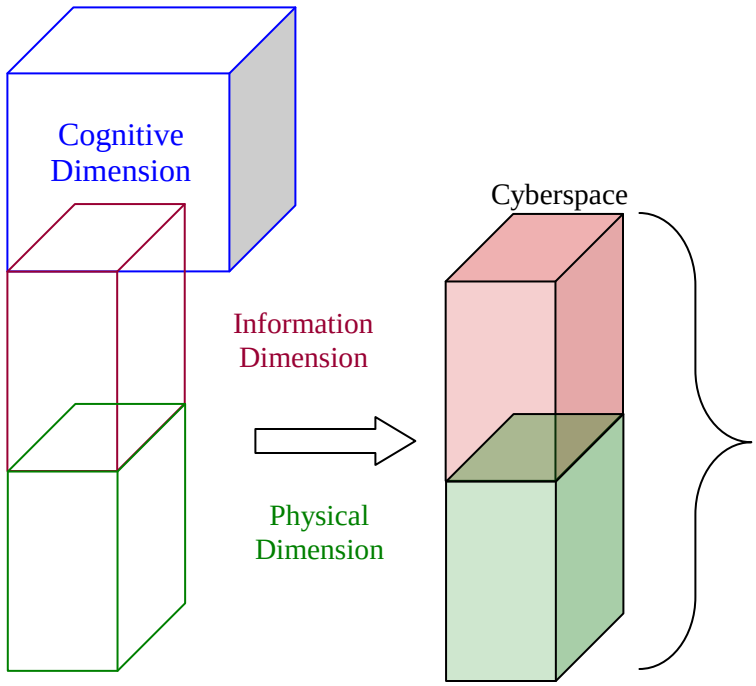



Cognitive Dimension
Where human decision making takes place
Dimension of intangibles such as morale, unit cohesion, public opinion, situational awareness
Key characteristics: perceptions, emotions, awareness, and understanding

Information Dimension
Where information is collected, processed, stored, disseminated, displayed, and protected
Dual nature - information itself and the medium
Links physical and cognitive dimensions
Key characteristics: information content and flow, information quality
Where automated decision making takes place

Physical Dimension
Where the information environment overlaps with the physical world
Information systems and networks
Key characteristics: computers and communications systems, and supporting infrastructures

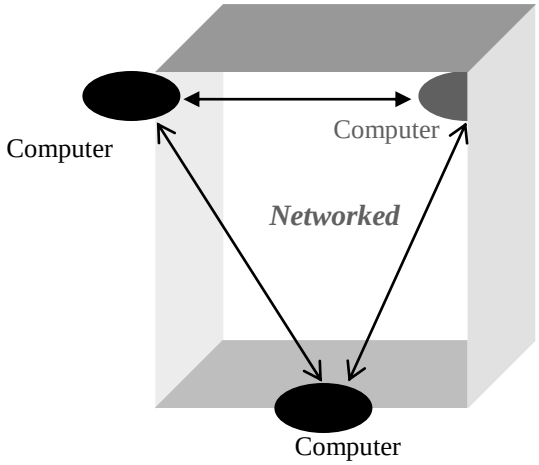
Cyberspace consists of part of the information environment. It primarily encompasses the physical (interconnected) dimension; this is a function of our interconnected world. Information that is exchanged through networks is also *created, modified and stored* through electronics and associated networks




Cyberspace is a subset of the Information Dimension and Physical Dimensions of the Information Environment.

[45] The visual depiction was borrowed from Army IO Primer, 2008, pg. 2; Definitions from JP3-13, pg. I-2.

**FIGURE 3: CYBERSPACE IS A PHYSICAL PLACE WHERE INNUMERABLE PARTIES CONNECT**




Cyberspace: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers

For the war fighter, this interdependent network of information technology infrastructures is a new kind of physical space through which an adversary may be connected. It can overlie the other domains wherever "connections" exist as per the cyberspace definition above.

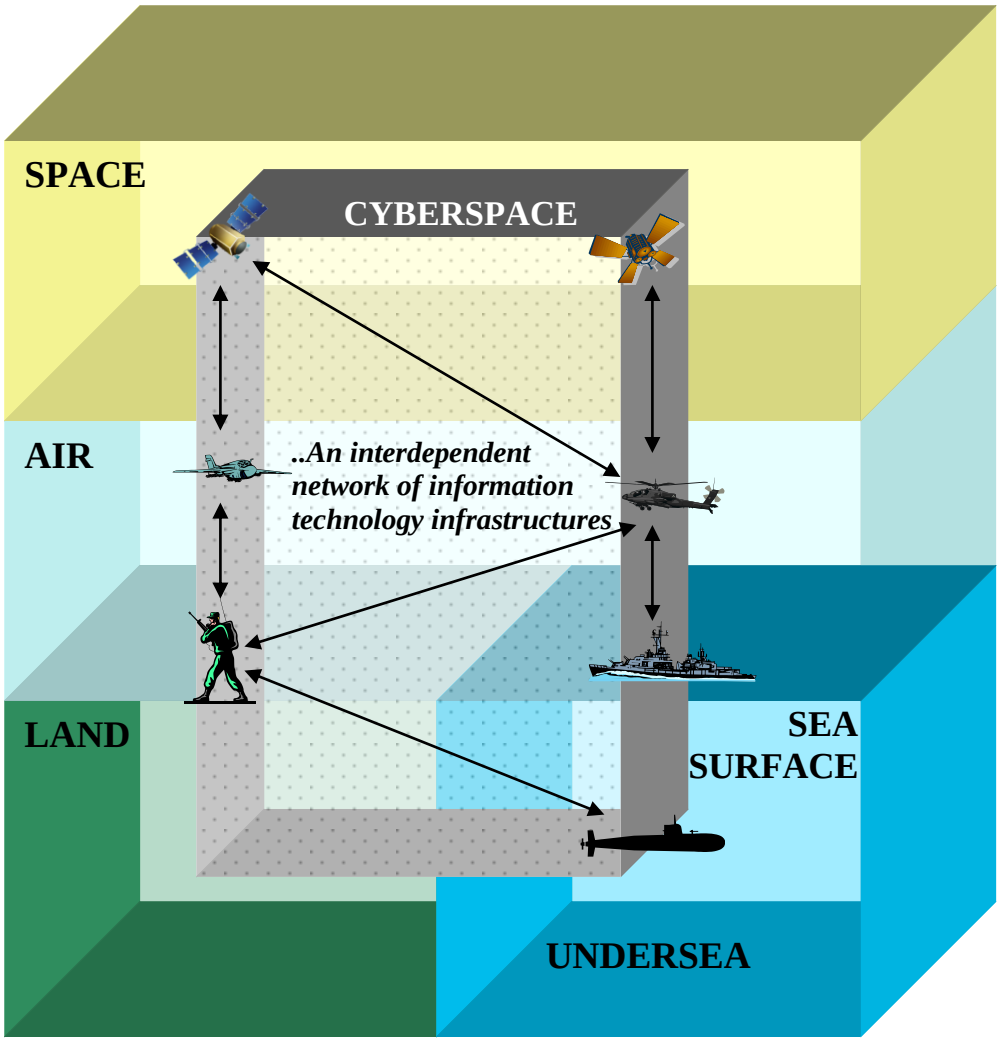


**FIGURE 4: PROPOSED COCOM ORGANIZATION WITH JFCYCC.**
This includes JFCyCC relationships with STRATCOM, JFCC/NW, and NSA.
This also depicts notional subordinate Joint Task Force.
J39 Highlighted for reference. Additional positions included for reference only.

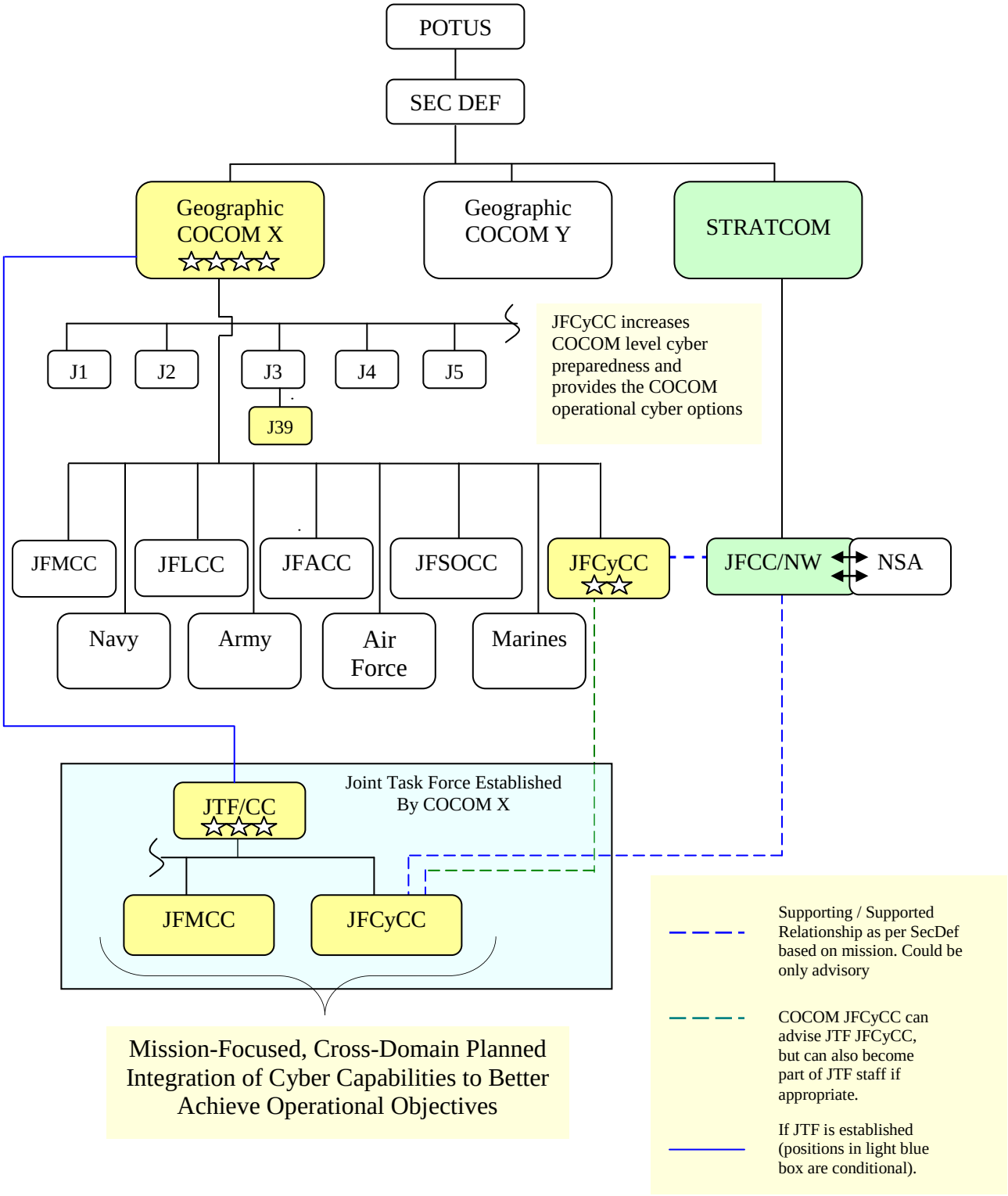


**FIGURE 5: JOINT CYBERSPACE COMPONENT COMMANDER ACHIEVES FREEDOM OF ACTION IN CYBERSPACE**

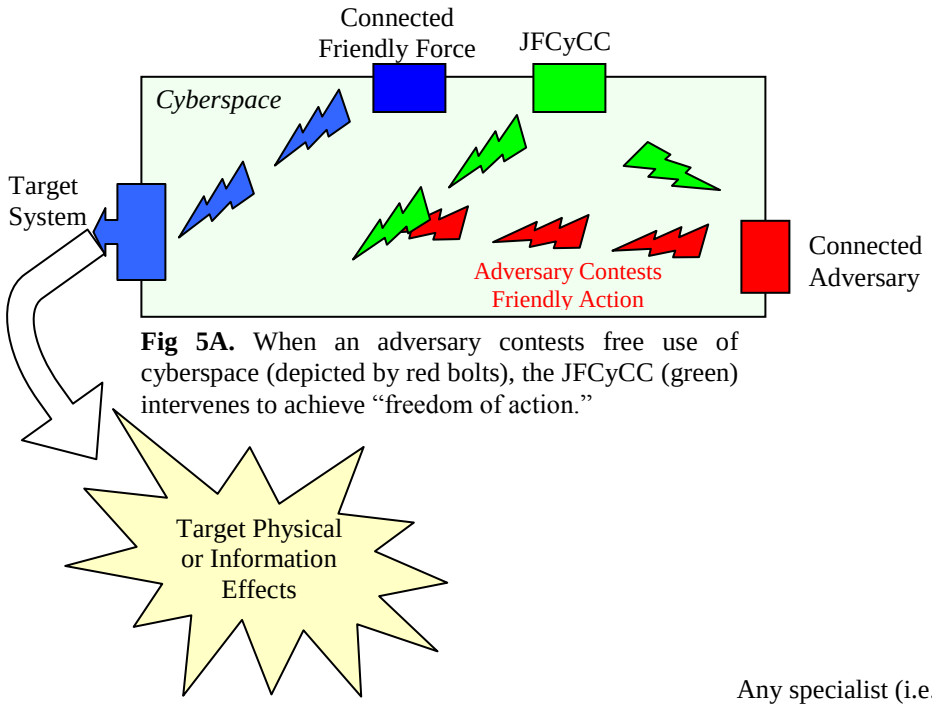



**Fig 5A.** When an adversary contests free use of cyberspace (depicted by red bolts), the JFCyCC (green) intervenes to achieve "freedom of action."

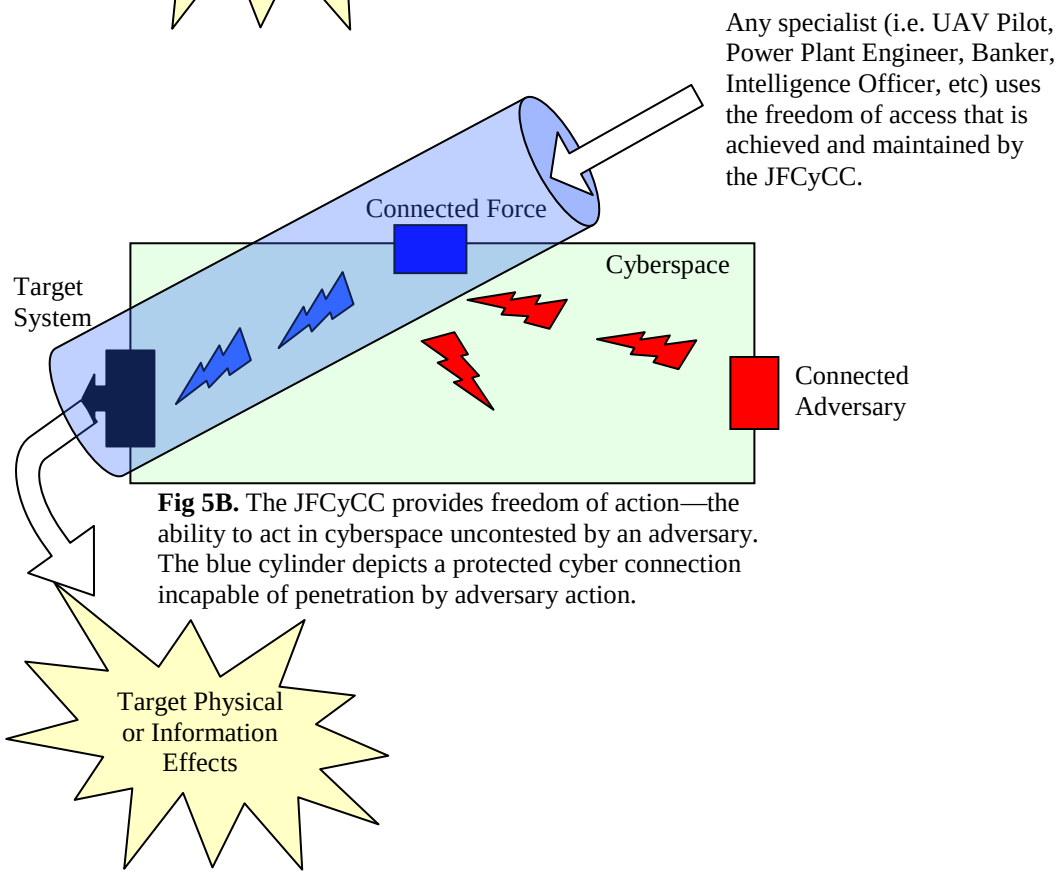



**Fig 5B.** The JFCyCC provides freedom of action—the ability to act in cyberspace uncontested by an adversary. The blue cylinder depicts a protected cyber connection incapable of penetration by adversary action.

# GLOSSARY

**Computer Network Attack (CNA): (JP 3-13):** actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.

**Computer Network Defense (CND): (JP 3-13):** actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks. Joint Pub 6.0 further outlines Computer Network Defense as an aspect of NetOps.

**Computer Network Exploitation (CNE): (JP 3-13):** enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

**Control System Attack (CSA):** is a type of CNA conducted through cyberspace intended to affect other networked objects, including, but not limited to supervisory control and data acquisition systems, surveillance, and kinetic weapons. A CSA generally creates destruction and is considered a use of force. Ex's include disrupting, damaging, or affecting fire control commands to weapons, military C2, & other physical world.[46]

**Coordinating Authority: (JP 1-02):** A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more military departments, two or more joint force components, or two or more forces of the same service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations.

**Cyberspace: (Gibson, 69):**A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. … A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding

**Cyberspace: (NMS-CO, 12/06):** "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."

**Cyberspace: (NSPD-54, 1/08)**: "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."

**Cyberspace: (Gordon England, DepSecDef 6/08):** "...a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."

**Information Operations (IO): (JP 3-13):** "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."

**Information system attack (ISA)**: A type of computer network attack intended to disrupt, corrupt, deny, degrade, or destroy information residing in, or transiting cyberspace where data itself is the target. ISA does not involve the use of force. Examples include deleting files, altering web pages, or fabricating emails.[47]

**SIGINT**: (Signals Intelligence) a category of intelligence that includes transmissions associated with communications, radars, and weapons systems used by our adversaries. (http://www.nsa.gov/sigint/index.shtml)

---

[46] Mark J. Matsushima, "*Words Mean Things: The Case for Information System Attack and Control System Attack*" (research paper, Newport, RI: U.S. Naval War College, JMO Department, 2008), 5-6.

[47] Ibid

## BIBLIOGRAPHY


Alexander, Keith B., "*Warfighting in Cyberspace*." Joint Forces Quarterly, no. 46 (3rd Quarter 2007): 58-61

Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (U), (Washington, DC: CJCS, September 2006), (Secret) Information extracted is unclassified, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 26 March 26, 2009).

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

CNO Strategic Studies Group (SSG), XXVI. *Convergence of Sea Power and Cyber Power.* Final Report delivered to Chief of Naval Operations, Washington, D.C., July 2007.

CNO Strategic Studies Group (SSG) XXVII. *Collaborate & Compel--Maritime Force Operations in the Interconnected Age.* Final Report delivered to Chief of Naval Operations, Washington, D.C., July 2008.

Convertino, et. al. *Flying and Fighting in Cyberspace*. Maxwell Paper No. 40. Maxwell AFB, AL: Air University Press, July 2007.

*Cyber Security and Monitoring. National Security Presidential Directive/NSPD-54).* (8 Jan 2008). (Secret) Information extracted is unclassified.

Elliott, Michael C., "*Operational Command and Control of Joint Task Force Cyberspace Operations*." (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008).

Gibson, William. *Neuromancer.* New York, NY: Ace Books, 1984.

Kuehl, Daniel. *From Cyberspace to Cyber Power: Defining the Problem.* Working Paper from National Defense University Center for Technology and National Security Policy's Workshop on Cyberpower. 2008. http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc. Accessed 24 Apr 09.

Mathers, Russell F., "*Cyberspace Coercion In Phase 0/1: How to Deter Armed Conflict*," Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007.

Matsushima, Mark J., "*Words Mean Things: The Case for Information System Attack and Control System Attack*" Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008.

Olsen, Kelly L., *Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative.* Research paper, Carlisle Barracks, PA: U.S. Army War College, 15 Mar 2008.

Porter, Michael E, *What is Strategy?* Cambridge, MA: Harvard University Press, November/December 1996.

U.S. Air Force. *Concept of Cyber Warfare*. Barkesdale AFB, LA: U.S. Air Force Cyber Command (P), 26 November 07.

U.S. Army. *Army IO Primer. Fundamentals of Information Operations.* U.S. Army War College. Carlisle, PA. Dec. 2007.

U.S. Department of Defense. *DoD Releases Unified Command Plan 2008*. News Release, 23 December 2008. http://www.defenselink.mil/releases/release.aspx?releaseid=12408. Accessed 24 April 29, 2009.

U.S. Department of Defense. *The Definition of "Cyberspace."* Washington, DC: Office of the Deputy Secretary of Defense, 12 May 2009.

U.S. General Accounting Office, *Information Security—Computer Attacks on the Department of Defense Pose Increasing Risks.* (Washington DC: Government Printing office, 22 May 1996).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations.* Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. President, *The National Strategy to Secure Cyberspace.* Washington, DC: White House, 2003.

U.S. Strategic Command. "Joint Information Operations Warfare" http://www.stratcom.mil/factsheets/jiowc/ (accessed 18 April 2009).

U.S. Strategic Command. *"Striking the Balance-Today's War, Tomorrow's threats, Future Technology"* Address. Air Force Association Convention, Orlando, FL, 8 Feb 2007. http://www.stratcom.mil/speeches/4/ (accessed 24 April 2009).

Vego, Milan. *Joint Operational Warfare: Theory & Practice*. Newport, RI: Naval War College Press, 2007.

Webster's Online Dictionary. "Domain." http://www.merriam-webster.com/dictionary/domain (accessed 12 April 2009).